UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/469,505	12/22/1999	ROBERT J. STONE	UUN99006	5044

25537 7590 03/31/2004

WORLDCOM, INC.
TECHNOLOGY LAW DEPARTMENT
1133 19TH STREET NW
WASHINGTON, DC 20036

EXAMINER	
LAFORGIA, CHRISTIAN A	
ART UNIT	**PAPER NUMBER**
2131	17

DATE MAILED: 03/31/2004

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/469,505	STONE ET AL.	
	Examiner	Art Unit	
	Christian La Forgia	2131	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *30 December 2003*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-29* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-29* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date *15*.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

1. The amendment filed on 30 December 2003 is noted and made of record.

2. Claims 1 through 29 are presented for examination.

Response to Arguments

3. Applicant's arguments with respect to claims 1-29 have been considered but are moot in view of the new ground(s) of rejection.

4. See further rejections that follow.

Claim Rejections - 35 USC § 103

5. The text of those sections of Title 35, U.S. Code not included in this action can be found in a prior Office action.

6. Claims 1-27 are rejected under 35 U.S.C. 103(a) as being unpatentable over U.S. Patent No. 6,687,732 to Bector et al., hereinafter Bector, in view of U.S. Patent No. 6,611,872 to McCanne, hereinafter McCanne.

7. As per claim 1, Bector teaches a method for tracking denial-of-service floods, the method comprising:

rerouting a DoS flood attack datagram to a tracking router (Figure 1 [blocks 107, 114]; column 4, lines 9-50; column 14, lines 3-31);

identifying an ingress edge router that forwarded the DoS flood attack datagram (column 4, lines 37-50). Bector teaches identifying the origin computer of the malicious content, thus if the origin computer can be identified the ingress edge router that received the malicious datagram can be identified. Bector discloses the present invention except for wherein the tracking router forms an overlay tracking network with respect to an egress edge router.

McCanne discloses that is known to use an overlay tracking network to track data over an intended path. It would have been obvious to one of ordinary skill in the art at the time the invention was made to have the proxy server form an overlay tracking network as taught by McCanne, since McCanne states at column 2, lines 40-66 that such a modification would allow the system to manage the denial of service attack more intelligent, bandwidth-efficient manner.

8. Regarding claim 2, Bector teaches further comprises executing security diagnostic functions (column 4, lines 9-50).

9. With regards to claims 3 and 15, Bector teaches wherein the security diagnostic functions comprise input debugging (column 4, lines 9-50).

10. Regarding claims 4 and 16, McCanne teaches wherein the overlay tracking network is within an autonomous system that is different from another autonomous system corresponding to the ingress edge router and the egress edge router (Figures 1, 2; column 6, line 65 to column 7, line 40).

11. With regards to claims 5, 11, and 17, McCanne teaches further comprising providing routing information by the overlay tracking network to the ingress edge router and the egress edge router using an inter-administrative-domain routing/signaling protocol (column 4, lines 52-66; column 17, lines 9-60).

12. Concerning claims 6, 12, and 18, McCanne teaches wherein the inter-administrative-domain routing/signaling protocol is BGP (Border Gateway Protocol) (column 4, lines 52-66; column 17, lines 9-60).

13. Regarding claims 7, 19, and 23, McCanne teaches further comprising communicating between the edge routers and the tracking router via tunnels that are created over an unreliable datagram delivery service protocol (column 4, lines 53-65; column 6, lines 11-26).

14. Regarding claims 8, 20, and 24, McCanne teaches further comprising communicating between the edge routers and the tracking router via virtual connections over a separate lower layer protocol (column 6, line 65 to column 7, line 32).

15. Regarding claims 9, 21 and 25, McCanne teaches further comprising communicating between the edge routers and the tracking router via physical connections (Figure 1 [access link]; column 7, lines 32-40).

16. Regarding claim 10, Bector teaches further comprising routing the DoS flood attack datagram from the ingress edge router to the tracking router, wherein the egress edge router has a static route to the victim (Figure 1 [blocks 107, 114]; column 4, lines 9-50; column 14, lines 3-31).

17. Concerning claims 13 and 27, Bector teaches further comprising establishing another static route between the egress router and an external router associated with a victim node, the victim node receiving the DoS flood attack datagram (column 8, line 50 to column 9, line 30).

18. As per claim 14, McCanne teaches a communication system for tracking denial-of-service (DoS) floods, the communication system comprising:

a plurality of edge routers including an ingress edge router and an egress edge router, (Figures 1, 2, 4a, 4b, 4c, 5; column 5, lines 29-63; column 16, line 66 to column 17, line 43);

a tracking router adjacent to the egress edge router, the tracking router being configured to perform the security diagnostic functions, (Figures 1, 2, 4a, 4b, 4c, 5; column 5, lines 29-63; column 16, line 66 to column 17, line 43). McCanne discloses the claimed invention except for each of the edge routers being configured to perform security diagnostic functions, in part, to identify a DoS flood attack datagram, wherein the ingress edge router is associated with a source of the DoS flood attack datagram and the ingress edge router rerouting the DoS flood attack datagram to the tracking router as to permit identification of the ingress edge router, wherein the tracking router forms an overlay tracking network with respect to the plurality of edge routers. Bector discloses that is its known for routers to perform security diagnostics, which include identifying a DOS attack, and rerouting the malicious datagram to an overlay network. It would have been obvious to one of ordinary skill in the art at the time the invention was made to include the security diagnostic functions as taught by Bector, since Bector states at column 4, lines 2-54 that such a modification would increase network security.

19. Regarding claim 22, McCanne teaches wherein the overlay tracking network further comprises additional tracking routers (column 7, lines 32-40).

20. Regarding claim 26, Bector teaches wherein the ingress edge router routes the DoS flood attack datagram to the tracking router due to a dynamic routing update from the tracking router (Figure 1 [blocks 107, 114]; column 4, lines 9-50; column 14, lines 3-31).

21. Claims 28 and 29 are rejected under 35 U.S.C. 103(a) as being unpatentable over Bector.

22. As per claim 28, Bector teaches a computer-readable medium carrying one or more sequences of one or more instructions for tracking denial-of-service floods (DoS), the one or more sequences of one or more instructions including instructions which, when executed by one or more processors, cause the one or more processors to perform the steps of:

receiving a DoS flood attack datagram (Figure 1 [blocks 107, 114]; column 4, lines 9-50; column 14, lines 3-31);

identifying the DoS flood attack datagram (Figure 1 [blocks 107, 114]; column 4, lines 9-50; column 14, lines 3-31);

identifying a previous hop router associated with the DoS flood attack datagram to ultimately locate an ingress adjacency and an ingress adjacency associated with the DoS flood attack (column 4, lines 37-50). Bector does not teach identifying previous hops. Bector teaches identifying the origin computer of the malicious content. It would have been obvious to one of ordinary skill in the art at the time the invention was made to locate the previous hops, since it has been held that Bector identifies the origin of the malicious datagrams.

23. Regarding claim 29, Bector teaches wherein the computer readable medium further includes instructions for causing the one or more processors to perform the steps of:

instructing the previous hop router to identify a respective previous hop router associated with the DoS flood attack datagram (column 4, lines 37-50). Bector does not teach identifying previous hops. Bector teaches identifying the origin computer of the malicious content. It would have been obvious to one of ordinary skill in the art at the time the invention was made to locate the previous hops, since it has been held that Bector identifies the origin of the malicious datagrams.

Conclusion

24. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

25. The following patents are cited to further show the state of the art with respect to detecting malicious datagrams, such as:

United States Patent No. 6,687,833 to Osborne et al., which is cited to show system for providing a network host decoy using a pseudo network protocol stack implementation.

United States Patent No. 6,363,489 to Comay et al., which is cited to show method for automatic intrusion detection and deflection in a network.

United States Patent No. 5,991,881 to Conklin et al., which is cited to show a network surveillance system.

United States Patent No. 6,578,147 to Shanklin et al., which is cited to show parallel intrusion detection sensors with load balancing for high speed networks.

United States Patent No. 6,609,205 to Bernhard et al., which is cited to show network intrusion detection signature analysis using decision graphs.

United States Patent No. 5,862,362 to Somasegar et al., which is cited to show network failure simulator.

26. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Christian La Forgia whose telephone number is (703) 305-7704. The examiner can normally be reached on Monday thru Thursday 7-5.

27. If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh can be reached on (703) 305-9648. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

28. Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Christian LaForgia
Patent Examiner
Art Unit 2131

clf

AYAZ SHEIKH
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100